European Ground System Architecture Workshop (ESAW)
May 10-11 2011

ARCHITECTURE GOVERNANCE

THE IMPORTANCE OF ARCHITECTURE GOVERNANCE FOR ACHIEVING OPERATIONALLY RESPONSIVE GROUND SYSTEMS

MIKE KOLAR (SPEAKER), JEFF ESTEFAN, BRIAN GIOVANNONI, ERIK BARKLEY

Topics

- Why Governance and Why Now?
- Characteristics of Architecture Governance
- Strategic Elements
  - Architectural Principles
  - Architecture Board
  - Architecture Compliance
- Architecture Governance Infusion Process

Why Governance and Why Now?

- "Governance" versus "Management"
  - Governance is concerned with decision making (i.e., setting directions, establishing standards and principles, and prioritizing investments)
  - Management is concerned with execution (i.e., how the actions resulting from decisions are executed)
- Growing relevance of software architectures is new and needs to be formalized
  - Executive forum necessary for planning and oversight of ground software architecture development
  - Will help insure effective introduction, implementation, and evolution of software architectures within the organization
- Breaking down of existing stovepipes and moving toward business agility
  - New ground system architectures need to be "composable" to meet broad spectrum of customer needs (large and small)
  - Growing body of value-added team collaboration—Program Offices, Line Organizations, CIO Office

Characteristics of Architecture Governance*

- Architecture governance is the practice and orientation by which enterprise architectures and other architectures are managed and controlled at an enterprise-wide level

- It is characterized by:
  - Implementing a system of controls over the creation and monitoring of all architectural components and activities, to ensure the effective introduction, implementation, and evolution of architectures within the organization
  - Implementing a system to ensure compliance with internal and external standards and regulatory obligations
  - Establishing processes that support effective management of the above processes within agreed parameters
  - Developing practices that ensure accountability to a clearly identified stakeholder community, both inside and outside the organization

**Source: The Open Group Architecture Framework (TOGAF), TOGAF 9, The Open Group, 2009.*

Strategic Elements*

- A comprehensive set of Architectural Principles should be established, to guide, inform and support the way in which an organization sets about fulfilling its mission through the use of information technology

- A cross-organizational Architecture Board must be established with the backing of top management to oversee the implementation of the architecture governance strategy

- An Architecture Compliance strategy should be adopted - specific measures (more than just a statement of policy) to ensure compliance with the architecture, including project impact assessments, a formal architecture compliance review process, and possibly including the involvement of the architecture team in product procurement

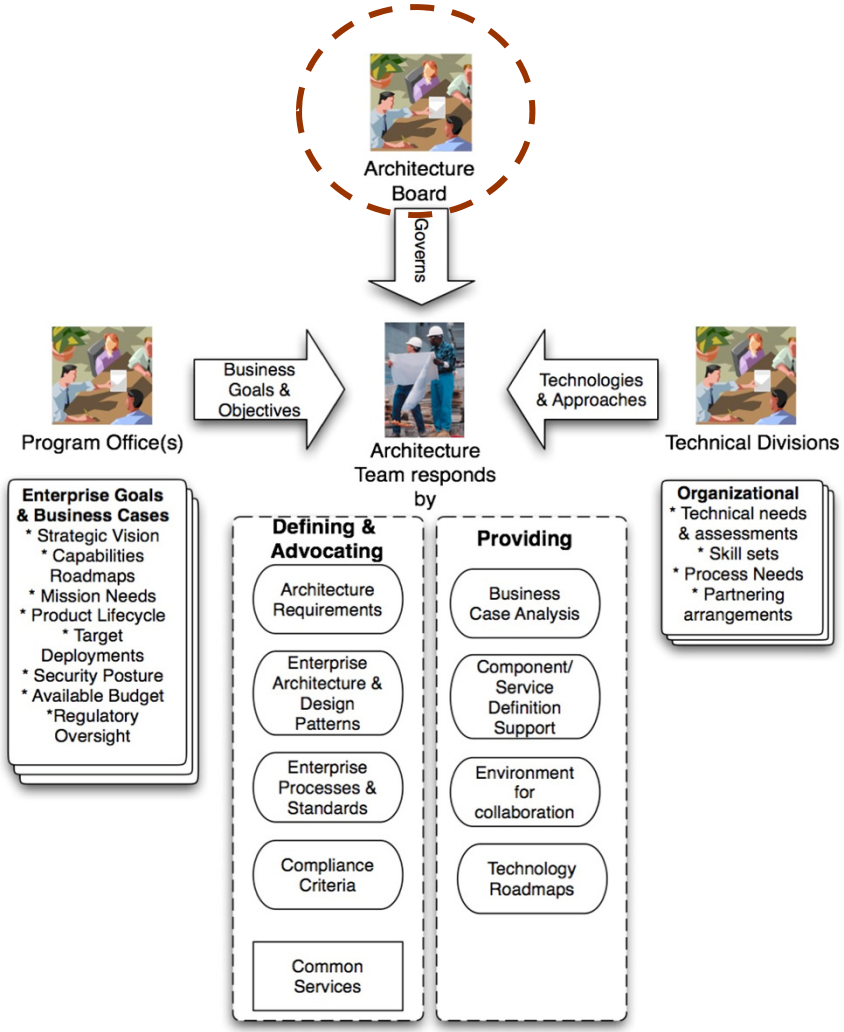
**Source: The Open Group Architecture Framework (TOGAF), TOGAF 9, The Open Group, 2009.*

Architectural Principles

- Architectural principles are a subset of IT Principles that relate to architecture work
- Architectural principles can be divided into principles that govern the architecture process and principles that govern the implementation of the architecture
- These principles (or tenets) can be mapped into a set of core technical areas in which
  - a roadmap for how capabilities can become compliant with the architecture can be provided, and
  - an objective measure of the capability's current state can be assessed

Architecture Board

- Purpose
  - Insure proposed ground software architectures benefit the Program(s), line or implementing organizations (Technical Divisions), and customer/user base
- Scope
  - Board should be comprised of ground software domain experts with line and programmatic (local) responsibility
  - Should also include members that have enterprise-wide (global) responsibility (e.g., CIO, DCIO, IT CTO)



Architecture Compliance

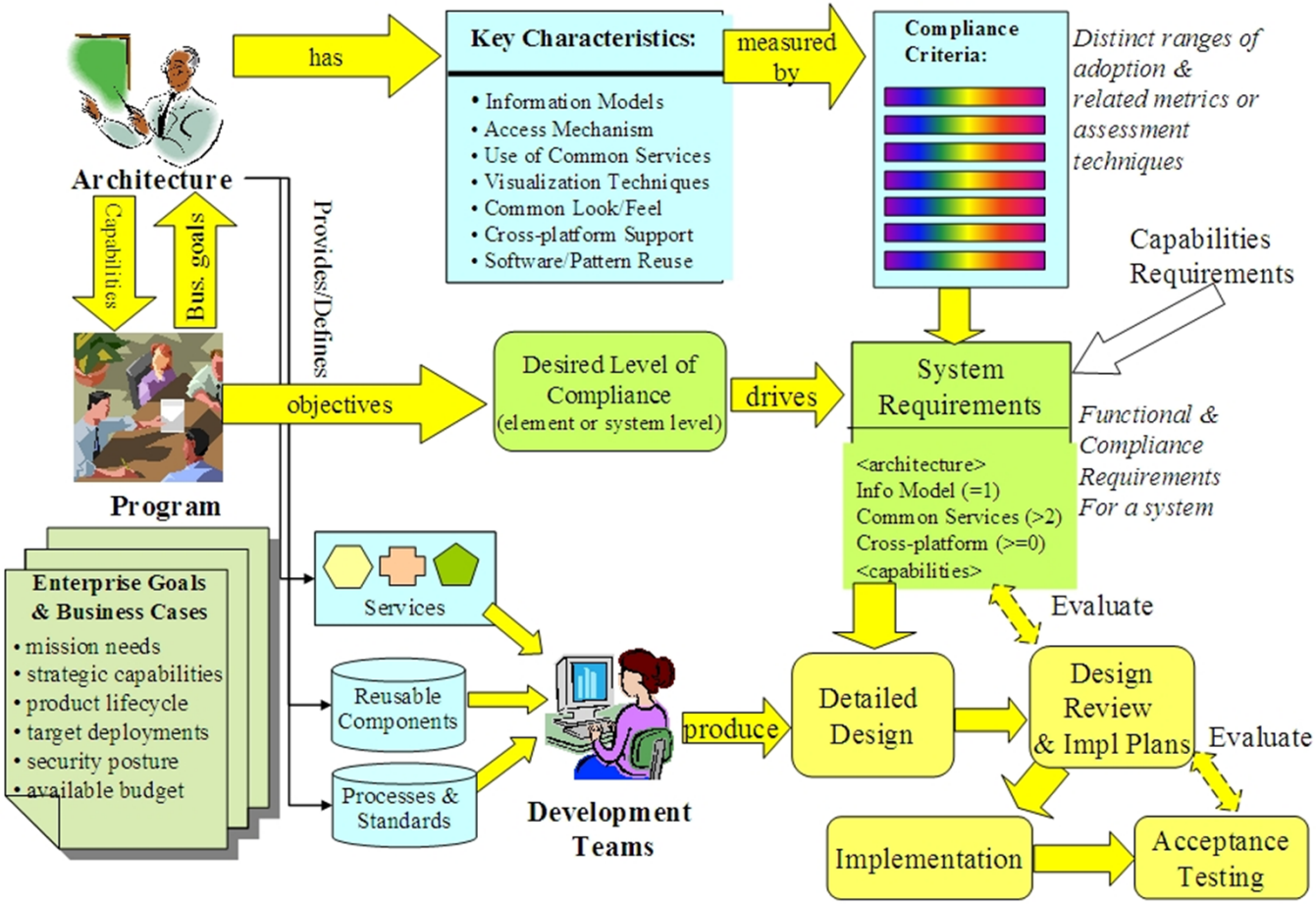
Objectives:

- Measure of how well an implementation conforms to key architectural and technical characteristics
- Helps provide an evolutionary roadmap and guide funding decisions

Areas of Compliance (example):

- √ Common Information Models
- √ Common Access Mechanisms
- √ Display Technology
- Common Display Look/Feel
- Cross Platform Support (Portability)
- Software Reuse
- Modularity
- Scalability
- Reliability
- √ Service Quality/Accountability
- Composability
- Deployability
- √ Security
- √ Storage
- Workflow
- √ Common Application Platform
- Network Utilization (adapts to directed or changes in network QoS)

Architecture Governance Infusion Process*



*Source: T. McVittie et al., "DSMS Software Architecture Review," Briefing Slides, JPL Internal Document, Jet Propulsion Laboratory, California Institute of Technology, Pasadena, CA, June 28, 2005

Summary

- Architecture Governance is the practice and orientation by which enterprise architectures and other architectures are managed and controlled at an enterprise-wide level
- Key strategic elements include: 1) establishment of a cross-organizational Architecture Board, 2) a comprehensive set of Architectural Principles, and 3) an the adoption of an Architecture Compliance strategy
- Architecture Governance will help insure effective introduction, implementation, and evolution of software architectures within the organization, including ground system architectures
- Essential to achieving operationally responsive ground systems

Backup

Hierarchies of Governance*

- Architecture governance typically operates within a hierarchy of governance structures:
  - Corporate Governance
  - Technology Governance
  - Information Technology (IT) Governance
  - Architecture Governance

- Each can have distinct domains with own disciplines and processes

- Each may exist at multiple geographic levels—global, regional, and local—within the overall enterprise

**Source: The Open Group Architecture Framework (TOGAF), TOGAF 9, The Open Group, 2009.*

Architectural Principles Template*

Name	***Should both represent the essence of the rule as well as be easy to remember. Specific technology platforms should not be mentioned in the name or statement of a principle. Avoid ambiguous words in the Name and in the Statement such as: "support," "open," "consider," and for lack of good measure the word "avoid," itself, be careful with "manage(ment)", and look for unnecessary adjectives and adverbs (fluff).***
Statement	***Should succinctly and unambiguously communicate the fundamental rule. For the most part, the principles statements for managing information are similar from one organization to the next. It is vital that the principles statement be unambiguous.***
Rationale	***Should highlight the business benefits of adhering to the principle, using business terminology. Point to the similarity of information and technology principles to the principles governing business operations. Also describe the relationship to other principles, and the intentions regarding a balanced interpretation. Describe situations where one principle would be given precedence or carry more weight than another for making a decision.***
Implications	***Should highlight the requirements, both for the business and IT, for carrying out the principle - in terms of resources, costs and activities/tasks. It will often be apparent that current systems, standards, or practices would be incongruent with the principle upon adoption. The impact to the business and consequences of adopting a principle should be clearly stated. The reader should readily discern the answer to "How does this affect me?" It is important not to oversimplify, trivialize, or judge the merit of the impact. Some of the implications will be identified as potential impacts only, and may be speculative rather than fully analyzed.***

**Source: The Open Group Architecture Framework (TOGAF), TOGAF 9, The Open Group, 2009.*

Architectural Principles (example)*

- ***4. Security**: Secure Federal information against unauthorized access.*
- Rationale: The Federal Government must be aware of security breaches and data compromise and the impact of these events. Appropriate security monitoring and planning, including an analysis of risks and contingencies and the implementation of appropriate contingency plans must be completed to prevent unauthorized access to Federal information. Information security must be ensured and increased, commensurate with increased access to Federal information.
- Implications: Protecting systems from spies, terrorists, and hackers requires considerable effort and costs. The business unit manager, where each system is implemented, must take responsibility for security measures and contingency plans as required by Presidential Decision Directive-63 (PDD-63), Critical Infrastructure Protection.

**Source: The Open Group Architecture Framework (TOGAF), TOGAF 9, The Open Group, 2009.*

Architecture Board Charter* (1/2)

- Operational & Programmatic Responsibilities
  - Insure consistency between sub-architectures (AMMOS and DSN)
  - Insure flexibility of architecture
    - to meet changing business needs
    - to leverage new technologies
  - Improve maturity level of architecture discipline within organization
  - Ensure discipline of architecture-based development is adopted
  - Provide basis for all decision making with regard to changes to the architectures
  - Support visible escalation capability for out-of-bounds decisions
- Governance Responsibilities
  - Produce usable governance material and activities
  - Determine which aspects of the architecture should be applied to particular capabilities and areas

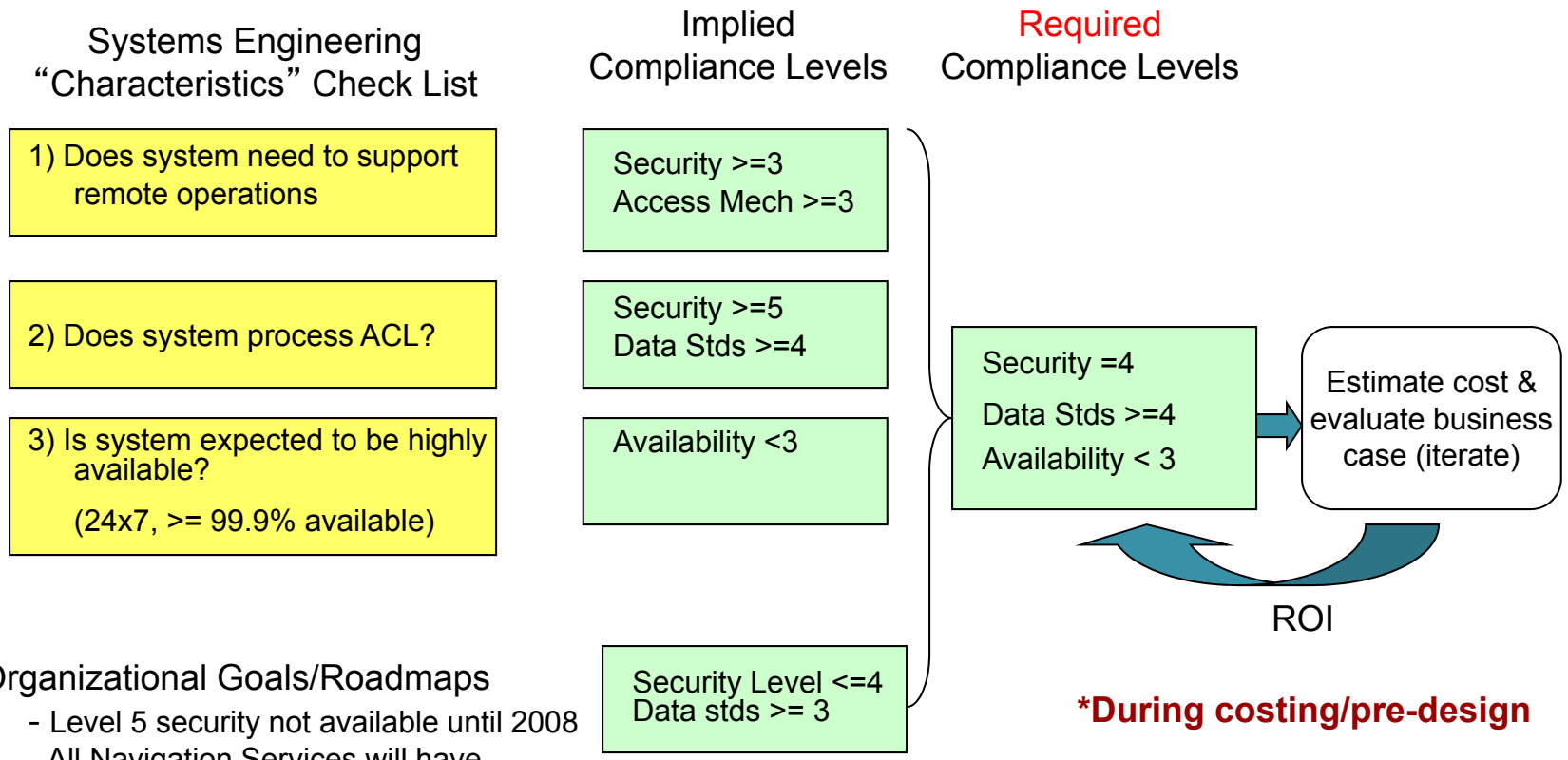
** Full scope and charter to be documented during inaugural meeting*

Architecture Board Charter (2/2)

- Governance Responsibilities (cont'd)
  - Review suitability of proposed service components of candidate capability areas to determine right level of granularity and identify any issues with respect to common services and COTS variants
  - Establish and maintain link between implementation of the architecture, architectural strategy and objectives embodied in the architecture, and strategic objectives reflecting business drivers
  - Assess levels of compliance to measure how well an implementation meets the intent of the architectural characteristics defined for specified target architecture

- Additional Responsibilities
  - Provide mechanism for formal acceptance and approval of architecture through consensus and authorized publication
  - Provide fundamental control mechanism for ensuring effective implementation of the architecture
  - Identify divergence from the architecture and planning activities for realignment through dispensations or policy updates

Establishing Required Compliance Levels*



- Approach allows us to determine the level of compliance required for an individual system based on its needed characteristics as well as organizational goals.
- Since levels are clearly associated with required capabilities, we can readily understand the impact of a waiver or need to support a new capability , e.g., if the system can only support a level 2 security capability, how will that impact the security of the enterprise?

Security Compliance Matrix (example)

Application's Current Compliance

Application's Target Compliance

Level 0 (none)
- Application utilizes no authentication or authorization mechanism
- Applications is available and gives identical rights to all users able to access the platform

Level 1 (application specific)
- Application authenticates users & controls what individual users can do.
- Application may provide its own identity and/or authorization capabilities

Level 2 (platform security)
- Application delegates responsibility for authentication and control over what a user can do to the underlying operating system
- Operating System (platform) provides identity services (logons), and authorization services (groups, ACLs, etc.)

Level 3 (external source)
- Application uses non-DISA supported external system as source of authentication and authorization.

Level 4 (uses local Security Services)
- Application uses DISA-provided security service to authenticate and authorize all access.

Well Defined Grouping of Capabilities

- Compliance Matrix provides a mechanism for mapping organizational goals and roadmaps onto the set of requirements. It allows us to think about these issues in a cross system context (vs on a case-by-case basis).
- Can also be used to measure where we are as well as define where we'd like to be.

Note: DISA = Deep Space Information Services Architecture